AMENDMENT

Amendments to the Claims

The claims are amended as shown on the following pages under the heading LIST OF CURRENT CLAIMS. The list shows the status of all claims presently in the application including any current amendments. This list of claims is intended to supersede all prior versions of the claims in the application. Any cancellation of claims is made without prejudice or disclaimer.

LIST OF CURRENT CLAIMS

1. (Currently Amended) A method for protecting data having an authentication phase comprising the following steps:

(a) providing a biometric feature;

(b) digitizing the biometric feature to create digitized biometric authentication feature data;

(c) decrypting an encrypted code word on the basis of the digitized biometric authentication feature data thereby obtaining a decrypted code word, and;

(d) recovering secret data from the decrypted code word on the basis of a coding-theory method ~~with a correction capacity, the correction capacity being freely selectable~~ within a freely selectable tolerance interval.

2. (Previously Presented) The method according to claim 1 having an initialization phase comprising:

after providing a biometric feature, digitizing the biometric feature to create digitized biometric feature data;

providing secret data;

encrypting on the basis of the digitized biometric feature data and fault tolerantly coding the secret data.

3. (Previously Presented) The method according to claim 2 including using the consecutive steps:

fault-tolerantly coding the secret data to create a code word;

encrypting the code word on the basis of the digitized biometric feature data to create an encrypted code word.

4. (Previously Presented) The method according to claim 3, wherein the code word is generated by a generating matrix.

5. (Previously Presented) The method according to claim 2 including the step of creating initial correction data to describe the space of allowed code words.

6. (Previously Presented) The method according to claim 2 including the step of providing initialization correction data on the basis of the digitized biometric feature data.

7. (Previously Presented) The method according to claim 1 including the steps:

creating authentication correction data on the basis of the digitized biometric authentication feature data;

recovering the digitized biometric feature data on the basis of the authentication and initial correction data;

decrypting encrypted secret data on the basis of the recovered digitized biometric feature data.

8. (Previously Presented) The method according to claim 7, wherein the initial correction data are created by calculation of the digitized biometric feature data modulo n.

9. (Previously Presented) The method according to claim 7, wherein the authentication correction data are created by calculation of the authentication feature data modulo n.

10. (Previously Presented) The method according to claim 2, including using user-specific initial correction data and/or user-specific fault-tolerant coding.

11. (Previously Presented) The method according to claim 2, wherein a public and a secret part are separated and determined or estimated from the biometric feature.

12. (Previously Presented) The method according to claim 11, wherein the separation into a public and a secret part of the biometric feature is effected with the aid of empirical inquiries.

13. (Previously Presented) The method according to claim 2, wherein a hash value is created from the digitized biometric feature data with the aid of a hash function.

14. (Previously Presented) The method according to claim 1, wherein a hash value is created from the digitized biometric authentication feature data with the aid of a hash function.

15. (Previously Presented) The method according to claim 1, wherein the biometric feature is a behavioral biometric.

16. (Previously Presented) The method according to claim 1, wherein the biometric feature consists of a handwritten signature.

17. (Previously Presented) The method according to claim 16, wherein the handwritten signature is broken down into a public and a secret part and the secret part is a proper subset of the dynamic information of the signature.

18. (Previously Presented) The method according to claim 1, wherein the providing and/or digitizing of the biometric feature is effected several times.

19. (Previously Presented) The method according to claim 1, wherein the secret data are generated with a public-key method.

20. (Currently Amended) An apparatus for protecting data, comprising:

digitizing apparatus arranged to digitize a biometric feature to thereby create digitized biometric feature data;

a secret data generator comprising;

apparatus arranged to fault-tolerantly code and decode the secret data; and

encrypting and decrypting apparatus arranged to encrypt and decrypt the fault-tolerantly coded secret data with the aid of the digitized biometric feature data~~.~~;

wherein an encrypted code word is decrypted on the basis of the digitized biometric feature data, thereby obtaining a decrypted code word and;

whereby the secret data is recovered from the decrypted code word on the basis of a coding theory method ~~with a freely selectable correction capacity~~ within a freely selectable tolerance interval.

21. (Previously Presented) The apparatus according to claim 20 including apparatus arranged to create code words.

22. (Previously Presented) The apparatus according to claim 20 including apparatus arranged to create initial correction data.

23. (Previously Presented) The apparatus according to claim 20 including apparatus arranged to provide a hash value.

24. (Previously Presented) The apparatus according to claim 20 including apparatus arranged to break down the biometric feature into a public and a secret part.

25. (Previously Presented) The apparatus according to claim 24 wherein the apparatus arranged to break down into a public and a secret part the biometric feature is further arranged to do so with the aid of statistical inquiries.

26. (Previously Presented) The apparatus according to claim 20, including apparatus arranged to capture a handwritten signature as a biometric feature.

In the claims

Claims 1 and 20 have been amended to replace the term "correction capacity" with the term "tolerance interval." The freely selectable tolerance interval is supported in the specification specifically in the last paragraph of page 13, and generally elsewhere in the specification such as discussion in the first full paragraph of page 14 of "the allowed variance of legitimate values."

It is respectfully submitted that none of the cited references disclose or suggest the claimed method (or apparatus) wherein secret data is recovered from a decrypted code word (the code word being decrypted on the basis of a digitized biometric authentication feature data) on the basis of a coding theory method within a freely selectable tolerance interval.

Conclusion

Every effort has been made to place the application fully in condition for allowance, and to remove all issues raised by the Examiner in the Official Action.

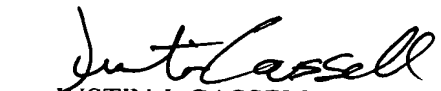
In view of the amendments to the claims, and in further view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is requested that claims 1-26 be allowed and the application be passed to issue.

If any issues remain that may be resolved by a telephone or facsimile communication with the Applicant's attorney, the Examiner is invited to contact the undersigned at the numbers shown.

Respectfully submitted,

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314-1176
Phone: (703) 683-0500

Date: August 11, 2006



JUSTIN J. CASSELL
Registration No. 46,205
Attorney for Applicant